DRAFT

US Government

Firewall Protection Profile

for

Sensitive but Unclassified Environments

Version 5.0

09 June 1997

DRAFT

Protection Profile Title:

US Government Firewall Protection Profile for Sensitive but Unclassified Environments.

Criteria Version:

This Protection Profile was developed using the guidance, constructs, conventions, and requirements of Version 1.0 of the Common Criteria (CCEB-96/012), dated 96/01/3 [1].

Constraints:

TOEs developed to satisfy this Protection Profile shall be CC Part 2 Conformant and CC Part 3 Conformant.

Authors:

This Protection Profile was prepared by:

Jack Walsh
National Security Agency

Jandria Alexander
The Aerospace Corporation

Mario Tinto
The Aerospace Corporation

Acknowledgements:

The authors would like to acknowledge the reviews and comments provided by Mike Hale, Kathy Dolan, and Tammy Mannarino of the National Security Agency and Lisa Carnahan, Barbara Guttman, and Wayne Jansen of the National Institute of Standards and Technology.

Table of Contents

Addendum

Conventions

The notation, formatting, and conventions used in this Protection Profile are largely consistent with that used in the Common Criteria, and with the example Protection Profiles of CCEB-96/014; “Part 4: Predefined Protection Profiles.” Selected presentation choices are discussed here to aid the reader.

Rationale is included in Protection Profiles as the vehicle for explicitly demonstrating that the set of requirements are complete relative to objectives; that each security objective (e.g., O.ACCESS) is addressed by one or more relevant requirements. As in the examples of the Common Criteria, this rationale is presented in its entirety in Section 6 of the Protection Profile.

As a further vehicle for providing understandability of and context for functional requirements, the notation Requirements Overview has been added to this Protection Profile. This provides a discussion of the relationship between functional requirements so that the reader can see why a group of requirements were chosen and what effect they are expected to have as a group of related functions. For instance, administrator capabilities are presented in the Common Criteria as a set of fine-grained and individually-selectable requirements, however, the intended global effect of a set of requirements needs to be understood. Such discussions precede the requirements that to which they are related. As an example, see the Requirements Overview in paragraph 5.1.1 of this Protection Profile (showing the relations between FDP_ACC, ADP_ACF, and FDP _ACF).

Application Notes are as used as an aid to the developer, either to clarify the intent of a requirement, identify implementation choices, or to define “pass-fail” criteria for a requirement. For an example, see the application notes associated with FDP_RIP.3 or ADV_RCR.1 of this Protection Profile.

The Common Criteria allows several operations to be performed on functional requirements; assignment, selection, and refinement, defined in paragraph 2.1.2 of Part 2 (i.e., CCEB-96/012). Each of these operations are used in this Protection Profile.

> The refinement operation is used to add detail to a requirement, and thus further restricts a requirement (e.g., restricting operations to an administrator). Refinement of functional requirements is denoted by **bold text**. For an example, see FIA_AFL.1 or FPT_TSA.2 of this Protection Profile.
>
> The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized*

text. For an example, see FAU_MGT.1 or FAU_STG.3 of this Protection Profile

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value]. For an example, see FDP_ACF.2 or FAU_SAR.3 of this Protection Profile.

The term “administrator” in this Protection Profile are meant to refer strictly to the administrator of the Firewall, and its use is not intended to include responsibilities for network administration.

Document Organization

Section 1 is the introductory material for the Protection Profile

Section 2 provides a general definition for firewalls and the expected architecture.

Section 3 is a discussion of the expected environment for the firewall, in particular the assumptions that must be true about aspects such as physical, procedural, and administrative controls. This section also defines the policies that are supported by a compliant firewall, and the set of threats that are to be addressed by either the technical countermeasures implemented in the firewall's hardware and software, or through the environmental controls.

Section 4 defines the security objectives for both the firewall and the environment in which the firewall resides.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the firewall.

Section 6 provides the mapping of requirements to the security objectives defined in Section 4. It represents an argument that each of the security objectives is satisfied through the successful implementation of one or more technical requirements.

Firewall Protection Profile

1 INTRODUCTION

1.1 IDENTIFICATION

1 Title: Firewall Protection Profile

2 Registration: <TBD>

3 Keywords: Access control, firewall, packet filter, network security, proxy servers, application gateway, protection profile.

1.2 PROTECTION PROFILE OVERVIEW

4 The intent of this protection profile is to specify features, mechanisms, and assurances applicable to firewalls. This profile specifies the minimum requirements for firewalls and is applicable to a variety of firewalls (e.g., combinations of proxy servers and packet filters on different platforms). It does not attempt to target any particular architecture or implementation. Rather, firewalls that provide all of the specified security features and assurances can be evaluated against this profile to determine compliance.

5 The purpose of a firewall is to provide a point of defense and a controlled and audited access to services, both from inside and outside an organization's private network, by permitting, denying, and/or redirecting the flow of data across the firewall.

6 The assurances for this Protection Profile are aimed at general commercial practice, with the primary purpose of demonstrating functional completeness. Thus the emphasis is on validation through testing, although some analysis is required for requirements that do not lend themselves easily to verification via testing (e.g., residual information protection, separation of domains of execution). Testing and high-level design documentation are relied upon as the primary vehicles for demonstrating functional completeness, functional correctness, and correspondence of implementation to design objectives.

7 The Application Notes section contains more details on the general model used in this profile.

1.3 RELATED PROTECTION PROFILES:

8 Network/Transport Packet Filter Protection Profile [2]

2 FIREWALL DESCRIPTION

9 The typical architecture of systems meeting this profile are described in Figure 2.1 below. The firewall is installed between internal and external networks so that traffic between them must be routed through the firewall. A firewall is one or more computing device. The firewall can thus provide access control between the hosts on different networks based upon either protocol header information or user information (when available), or both. A firewall is a computing device(s) (i.e., routers or hosts) that is used to physically separate one network domain from another.

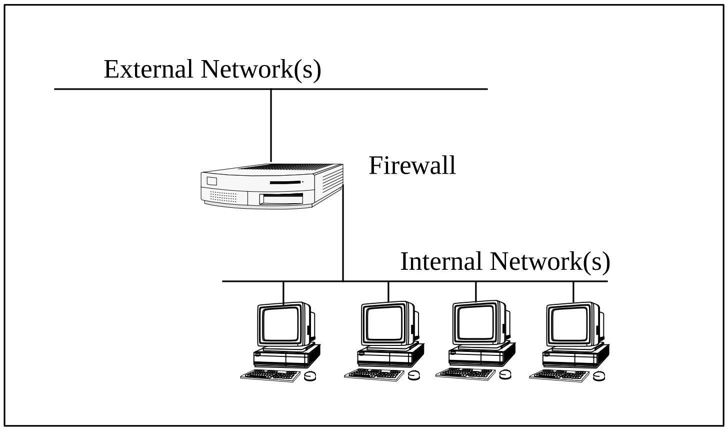

Figure 2.1 - Typical Firewall Location in Network

10 An example would be a firewall that performs security decisions based on information in both IP and TCP headers (e.g., source address and port) and is capable of providing user authentication. Firewall applications that run on multiple platforms should be evaluated on a particular platform, including both hardware and software, to meet the requirements stated in this protection profile. The protection profile is not intended to be used to evaluate applications separate from the platform and operating system.

3 SECURITY ENVIRONMENT

11 PP-compliant products are intended for use in environments for which access control decisions based upon US DoD labeled information (i.e., a multilevel

information policies) are not supported. Thus, either the firewall will be used in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is the same. Firewalls compliant with this Protection Profile provide access control policies, some auditing capability, and a low level of assurance.

12 The functional requirements in this profile fall into one of three categories:

a) those that are levied on session-oriented, interactive functions of the firewall;

b) those that are levied on non-session oriented, interactive functions of the firewall;

c) those that are levied on the firewall as a whole.

13 Some functional requirements in this profile are interpreted differently depending on whether “session-oriented” or “non-session-oriented” functions apply. Session-oriented functions include all services recognized by the firewall that support interaction with a user. These functions are characterized by the scenario of a human, either locally or remotely, making a request to a host being protected by the firewall (including the firewall itself), and expecting an interactive response. Examples of functions for which these requirements are intended to apply are Telnet, File Transfer Services (e.g., FTP), Web services, and firewall administrative or management services. For session-oriented requirements to be applied, the firewall must be “cognizant” of the session being established, (i.e., “cognizant” of a user).

14 Non-session-oriented functions include all other services supported by the firewall. “Store and forward” services, such as email, fall into this category.

15 The inclusion of requirements for session-oriented, as well as non-session-oriented, functions allows different types of firewall products to be evaluated using this profile. The non-session-oriented requirements will typically be applied to packet filter firewalls (generally offering non-session-oriented access control), while the session-oriented requirements apply to application gateway firewalls (which offer session-oriented access control). The profile also allows “hybrid” products which incorporate session and non-session-oriented services to be evaluated. Functional requirements of the firewall as a whole are those that apply to the composite system to include all services and functions. Example requirements that fall into this category include protection of the Target Of Evaluation (TOE) from interference or tampering.

3.1 SECURE USAGE ASSUMPTIONS

16 The following specific conditions are assumed to exist in the operational environment.

3.1.1 CONNECTIVITY ASSUMPTIONS

17 It is assumed that the following connectivity conditions exist:

A.SINGLEPT Single entry point

18 The firewall will be the only interconnection point between networks, as shown in the following figure.

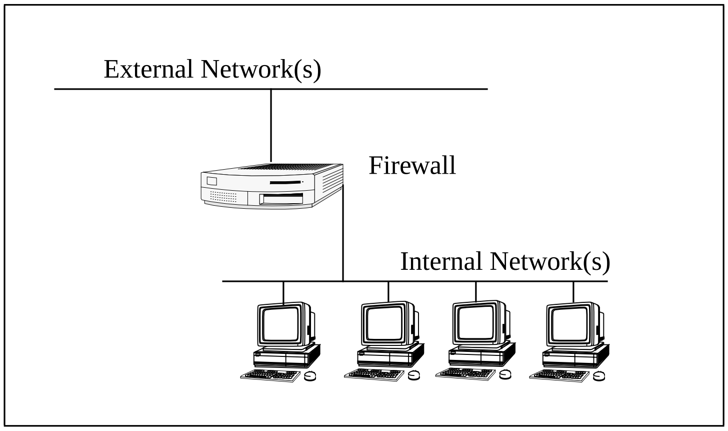

Figure 3.1 - Allowable Connections for PP-Compliant Firewalls

3.1.2 PHYSICAL ASSUMPTIONS

19 It is assumed the following physical conditions will exist:

A.SECURE Control of physical access

20 The firewall and associated directly-attached console is physically secure and available to authorized personnel only.

A.COMMS Protection of communications

21 The level of protection of any information transmitted is either protected commensurate with the level of information being transmitted (e.g., via physically protected transmission media, encryption), or an explicit judgment has been made that the information may be transmitted as plaintext.

3.1.3 PERSONNEL ASSUMPTIONS

22 It is assumed that the following personnel conditions will exist:

A.USER User services

23 The firewall only provides limited services (i.e., identification and authentication services) to network users. Firewall administrators have direct access and may also have remote access.

A.NOEVIL Trustworthy administrators

24 Administrators are assumed to be non-hostile, and trusted to perform their duties correctly.

3.2 ORGANIZATIONAL SECURITY POLICIES

25 This Protection Profile defines a product that is capable of enforcing restrictions on the flow of traffic both into and out of a local network. Traffic can be allowed, blocked or redirected based upon:

- ID of a host on an external network
- ID of a specific user on an external network
- ID of a host on an internal network
- Service(s) being requested (e.g., telnet, ftp).

26 PP-compliant products are considered to be suitable to provide protection in environments in which sensitive-but-unclassified information is being processed, or in which the networks being separated are all processing information at the same, single level. They are not intended to provide protection in multi-level environments.

27 The firewall security policy referred to in this document refers to the general security policy that a firewall supports rather than a site-specific policy that is tailored to specific organizational requirements.

3.2.1 THREATS TO SECURITY

28 This protection profile is sufficient for operational environments in which the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low. The intent of this profile is to control access to services, thereby limiting the

ability of unsophisticated, malicious users to gain access to the protected network or networks. To defend against more sophisticated attacks, such as IP spoofing or session hijacking, firewalls meeting this profile should be augmented with other security mechanisms or products to counter these threats.

3.2.2 THREATS ADDRESSED BY THE FIREWALL

29 The threat possibilities discussed below are addressed by pp-compliant firewalls.

T.LACCESS An unauthorized person may gain logical access to the firewall.

30 The term unauthorized person is used to cover all those persons who have, or may attempt to gain access to the system, but are not authorized users of the firewall.

T.SPOOF Network address spoofing attacks (e.g., IP spoofing) from one network connection to another, traversing the firewall.

31 The general model used is that the firewall provides access control between one or more “external” (untrustworthy) networks, and one or more “internal” (or “private”, trustworthy) networks. The specific threat countered is a subject on an external network attempting to masquerade as a subject on an internal network.

T.SACCESS Attacks on services.

32 The specific threats countered are a function of which protocols are allowed to pass through the firewall; a service that cannot be accessed from outside the network it is on does not pose a threat (other than threats originating inside a particular network, which are specifically not addressed in this profile) to that network, but it likewise is unusable by those outside that network.

T.PENET Undetected penetration attempts

33 An attacker may be able to attempt different attacks repeatedly against a network without personnel on the network under attack being aware that such attempts are taking place.

T.AUDITREV Lack of audit trail review.

34 Even if audit data are collected, if these data are not reviewed, either because of the quantity of data generated or lack of adequate review tools, an attacker may be able to escape detection while performing repeated penetration attempts.

T.ACORRUPT Corruption of audit trail by attacker.

35 The threat is two-fold. First, the attacker could directly corrupt the audit trail by manipulating it through an interface (e.g., a special firewall-specific control protocol going over the network) at the firewall. The second threat is that the attacker could crash the system after committing a penetration or attempted penetration, and if the audit data were not sufficiently protected it could be lost, thus masking the attacker's actions.

T.DCORRUPT Modification of firewall configuration and/or other security-relevant data.

36 This threat is similar to T.ACORRUPT, except that the data that are targeted by the attacker are firewall configuration and other security-critical data.

3.2.3 THREATS TO BE ADDRESSED BY OPERATING ENVIRONMENT

37 The threat possibilities discussed below are *not* addressed by pp-compliant firewalls. They must either be countered by the environment, procedural means, or accepted as potential system risks.

T.EVILADMIN Careless, wilfully negligent or hostile system administration personnel.

38 Since administrators are responsible for setting the access control rules and for monitoring the audit log, they will be able to trivially circumvent the security mechanisms of the firewall.

T.INSHARE Hostile users on a protected network ("inside" the firewall) attempting to give information to users on an external network.

39 This threat deals with the case that a user on an internal (protected) network attempts to send information to an unauthorized user on an external network. Since firewalls are basically designed to protect internal networks from external networks, they will be generally ineffective against these kinds of threats.

T.INALL Hostile users on a protected network attack machines also on the protected network.

40 Because a firewall by design is primarily to protect users on a network "inside" the firewall from users external to the firewall, it cannot control traffic that does not cross the firewall. Attacks falling in this category come from attacks on network services originating within the protected network, and targeting machines on that same network segment.

T.SERVICES Sophisticated attacks on higher-level protocols and services

41 These types of attacks target bugs in protocol layers (and services using those protocols, e.g., http) above the transport layer. PP-compliant firewalls may be able to completely deny access to specific services, but if packets are allowed to pass, then attacks on the services they are targeted for are possible.

T.PRIVACY Interception of transmitted information to acquire sensitive information.

42 Although a firewall may include support for cryptography, this is a class of problem that is commonly considered to fall outside the domain of responsibility of the firewall. Such attacks are usually countered via the use of protected communications channels or through the use of link or end-to-end encryption.

4 SECURITY OBJECTIVES

4.1 IT SECURITY OBJECTIVES

43 The following are the IT security objectives for the firewall:

O.ACCESS Access Mediation

44 The desire is to provide controlled access between networks connected to the firewall by permitting or denying the flow of information from a subject (sending entity) to an object (receiving entity) based on the attributes of the subject, object, possibly firewall-generated state information, and administratively configured access control rules.

O.ADMIN Administrator Access

45 This objective seeks to limit access to the firewall to authorised, administrative personnel, and to give only those individuals the ability to configure the firewall. This objective is closely related, and supports, O.AUDIT.

O.IDENT Individual Accountability

46 Individual identity seeks to provide user accountability and allows access decisions to be made based on this identity. Authentication provides a means to establish the validity of the claimed identity.

O.MINRES Minimum Direct Access

47 In order to meet this objective, the firewall must minimize direct resource availability for non-administrative users.

O.PROTECT Firewall Self-Protection

48 In order to successfully meet this objective, the firewall must be able to separate data that it needs to operate from data that it is processing. It must protect itself from attacks by external entities.

O.AUDIT Auditing

49 An audit trail is vital to determining if there are on-going attempts to circumvent the implementation of the security policy, or if there are mis-configurations of the firewall that unwittingly allow access where it should be denied. Not only must the audit data be collected, but it must be viewable and relatively easy to work with. Finally, the audit trail must be sufficiently protected and the scope of potential audit record loss known so that sound security decisions by administrative personnel can be supported.

4.2 NON-IT SECURITY OBJECTIVES

50 These are the objectives that are to be satisfied without imposing technical requirements on the firewall. That is they will not require implementation of mechanisms in the firewall hardware and/or software. Thus, they will be satisfied largely through application of physical, procedural, or administrative measures.

51 The firewall is assumed to be complete and self-contained and, as such, is not dependent upon any other products to perform properly. However, certain objectives with respect to the operating environment must be met in order to support the firewall’s security capabilities.

52 The following are the PP non-IT security objectives:

O.INSTALL Installation and Operational Controls

53 To ensure that the firewall is delivered, installed, managed and operated in a manner which maintains the system security.

O.PACCESS Physical Controls

54 Physical access to the firewall is controlled.

O.TRAIN Administrative Controls

55 Administrators are trained as to establishment and maintenance of sound security policies and practices.

5 IT SECURITY REQUIREMENTS

5.1 FIREWALL IT SECURITY REQUIREMENTS

56 This section provides functional and assurance requirements that must be satisfied by a pp-compliant firewall. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3.

5.1.1 FUNCTIONAL SECURITY REQUIREMENTS

57 The functional security requirements for this PP consist of the following components from Part 2, summarized in the following table:

Functional Class	Functional Components
User Data Protection	FDP_ACC.2,[a] Complete Object Access Control
	FDP_ACF.2, Multiple Security Attribute Access Control
	FDP_ACF.4, Access Authorization and Denial
	FDP_RIP.3, Full Residual Information Protection on Allocation
	FDP_SAM.1, Administrator Attribute Modification
	FDP_SAQ.1, Administrator Attribute Query

Table 5.1 - Functional Security Requirements

Identification and Authentication	FIA_ATA.1, User Attribute Initialization
	FIA_ADA.1,[a] User Authentication Data Initialization
	FIA_AFL.,1[a] Basic Authentication Failure Handling
	FIA_ADP.1,[a] Basic User Authentication Data Protection
	FIA_ATD.2,[a] Unique User Attribute Protection
	FIA_SOS.2, TSF Generation of Secrets
	FIA_UAU.2,[a] Single-use Authentication Mechanism
	FIA_UID.2, Unique Identification of Users
Protection of the Trusted Security Functions	FPT_RVM.1, Non-Bypassability of the TSP
	FPT_SEP.1, TSF Domain Separation
	FPT_TSA.2, Separate Security Administrative Role
	FPT_TSM.1, Management Functions
Security Audit	FAU_GEN.1, Audit Data Generation
	FAU_MGT.1, Audit Trail Management
	FAU_POP.1, Human Understandable Format
	FAU_PRO.1, Restricted Audit Trail Access
	FAU_SAR.1, Restricted Audit Review
	FAU_SAR.3, Selectable Audit Review
	FAU_STG.3, Prevention of Audit Data Loss

Table 5.1 - Functional Security Requirements

[a] *The specifics of these requirements are determined by whether they apply to session-oriented or non-session oriented functions. The function-related effect is addressed either as part of the requirement statement or in an associated Application Note. In most cases, a requirement will apply to only administrators in the case of non-session oriented functions, and apply to both general users and administrators for session-oriented functions.*

Requirements Overview:The first three requirements below (i.e., FDP_ACC.2, FDP_ACF.4, and FDP_ACF.2) provide the fundamental definitions for the firewall related to the enforcement of security policy. They define the entities (i.e., subjects and objects) that are recognized by the firewall, the access control rules (or "policy") that controls the access of subjects to objects, and the granularity of control that must be supported.

FDP_ACC.2 Complete Object Access Control

58 FDP_ACC.2.1 The TSF shall enforce the [firewall security policy, **FIREWALL_POLICY**][1], on:

a) The subjects: [hosts (source address) and users in the case of session-oriented functions; hosts (source address) for non-session oriented functions].

b) The objects: [hosts and services].

and all operations among subjects and objects covered by the SFP.

59 FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object in the TSC are covered by the Security Function Policy (SFP).

Application Note: The ST shall identify the specific operations that are provided, and specify how they are mediated by the SFP. Minimally, requests for access between hosts or users and hosts shall be mediated. However, the firewall developer may also choose to control access at the level of the service requested (e.g., ftp) or on specific service requests (e.g., "put," "get"). The ST must specify the granularity at which access control is performed, and which operations are covered by the SFP.

FDP_ACF.4 Access Authorization and Denial

60 FDP_ACF.4.1 The TSF shall enforce the [firewall security policy, **FIREWALL_POLICY**], to provide the ability to explicitly grant access based on the value of security attributes of subjects and objects.

61 FDP_ACF.4.2 The firewall shall enforce the [firewall security policy, **FIREWALL_POLICY**], to provide the ability to explicitly deny access based on the value of security attributes of subjects and objects.

[1] The firewall security policy, designated as "FIREWALL_POLICY" is essentially defined by the requirements articulated in FDP_ACC.2, FDP_ACF.4, and FDP_ACF.2.

FDP_ACF.2 Multiple Security Attribute Access Control

62 FDP_ACF.2.1 The TSF shall enforce the [firewall security policy, **FIREWALL_POLICY**], on objects based on [subject identity, object identity, role[2], and location (i.e., internal or external to the protected network)].

63 FDP_ACF.2.2 The TSF shall enforce the following **additional** rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) [The firewall shall reject requests for access or services that originate from one side of the network, but which have the source address of a host on the other side].

b) [The firewall shall allow administrator access only to those specific users authorized to invoke that role].

FDP_RIP.3 Full Residual Information Protection on Allocation.

64 FDP_RIP.3.1 The TSF shall ensure that upon the allocation of a resource to all objects any previous information content is unavailable.

Application Note: This requirement deals with the need to manage all resources (e.g., registers, buffers) used to support connections such that no network user has access to information from previous sessions. Thus, no message or session segment should contain information from any other network user’s communications. This requirement is usually satisfied via clearing or overwriting of such resources.

Requirements Overview:The next two requirements (i.e., FDP_SAM.1, FDP_SAQ.1) identify the capabilities required to support the administrator role, specifically the capability to review and modify security-related parameters. These are elaborated on or augmented in following requirements that deal with the need for the firewall to support the initialization of several security-related data. The requirements that follow, from class FIA, are closely related and largely deal with the need for defining, managing, and using security-related parameters, such as authentication data.

FDP_SAM.1 Administrator Attribute Modification

65 FDP_SAM.1.1 The TSF shall enforce the *access control SFP* to provide authorized administrators with the ability to modify:

- [The association of User IDs with roles (e.g., administrator)];

[2] *The only roles that must be supported in a pp-compliant firewall are those of administrative and non-administrative users.*

- [Manage security-relevant databases].

FDP_SAQ.1 Administrator Attribute Query

66 FDP_SAQ.1.1 The TSF shall enforce the _access control SFP_ to provide the authorized administrator with the ability to query [host names, host locations and addresses, user names, services and applications].

FIA_ADA.1 User Authentication Data Initialization

67 FIA_ADA.1.1 The TSF shall provide functions for initializing user authentication data related to [authentication mechanisms identified in FIA_UAU.2].

68 FIA_ADA.1.2 The TSF shall restrict use of these functions to the authorized administrator.

Application Note: This requirement applies as stated for session-oriented functions. In the case of non-session oriented non-session oriented functions, user identity is typically not known. Therefore, for firewalls that support only non-session oriented functions and thus do not maintain authentication data for non-administrative users, the requirement is applied only to authentication data for administrators.

FIA_ADP.1 Basic User Authentication Data Protection

69 FIA_ADP.1.1 The TSF shall protect from unauthorized observation, modification, and destruction authentication data that is stored in the TOE.

Application Note: For firewalls that support only non-session oriented functions and thus do not maintain authentication data for non-administrative users, the requirement is applied only to the protection of authentication data for administrators.

FIA_AFL.1 Basic Authentication Failure Handling

70 FIA_AFL.1.1 The TSF shall be able to terminate the user session establishment process after [a settable number] of unsuccessful authentication attempts. **The failure threshold shall be settable only by an authorized administrator.**

Application Note: For a firewall, the use of the term “session” is taken to mean user account or host account

71 FIA_AFL.1.2 After the termination of the user session establishment process the TSF shall be able to disable the *user or host session* until [the session is unblocked by the authorized administrator].

Application Note: For firewalls that support only non-session oriented functions and thus do not maintain authentication data for non-administrative users, the requirement is applied only to attempted administrator activities.

FIA_ATA.1 User Attribute Initialization

72 FIA_ATA.1.1 The TSF shall provide the ability to initialize user attributes with provided default values.

Application Note: For firewalls supporting only non-session oriented functions, this requirement applies only to administrator attributes.

FIA_ATD.2 Unique User Attribute Definition

73 FIA_ATD.2.1 The TSF shall provide, **for each user that is defined to it**, a unique set of security attributes necessary to enforce the TSP.

Application Note: For firewalls supporting only non-session oriented functions, this requirement applies only to administrator attributes.

FIA_SOS.2 TSF Generation of Secrets

74 FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [any of the standards identified in Appendix A.]

75 FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [FIA_UAU.2 Single-use Authentication Mechanism].

FIA_UAU.2 Single-use Authentication Mechanisms

76 FIA_UAU.2.1 The TSF shall authenticate any user’s claimed identity prior to performing any functions for the user.

77 FIA_UAU.2.2 The firewall shall prevent reuse of authentication data, **except in the case of users performing system administration via a directly-connected console in which case reusable passwords are sufficient**.

Application Note: For firewalls supporting only non-session oriented functions, this requirement applies only to the authentication of administrators.

FIA_UID.2 Unique Identification of Users

78 FIA_UID.2.1 The TSF shall uniquely identify each user before performing any actions requested by the user.

Requirements Overview:The next two requirements (i.e., FPT_RVM.1 and FPT_SEP.1) deal with the fundamental architectural ability to protect its internal code and data structures, and to be able to demonstrate that the security policy is always invoked.

FPT_RVM.1 Non-Bypassability of the TSP

79 FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before any security-related operation is allowed to proceed.

FPT_SEP.1 TSF Domain Separation

80 FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

81 FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Application Note: For those cases in which the firewall contains only security-relevant functions (i.e., supports no untrusted user processes), the requirement for a separate domain is trivially met.

FPT_TSA.2 Separate Security Administrative Role

82 FPT_TSA.2.1 The TSF shall distinguish security-relevant administrative functions from other functions.

83 FPT_TSA.2.2 The TSF's set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TSF; minimally, this set shall include [add and delete subjects and objects; view security attributes; assign, alter, and revoke security attributes; review and manage audit data].

84 FPT_TSA.2.3 The TSF shall restrict the ability to perform security-relevant administrative functions to a security administrative role that has a specific set of authorized functions and responsibilities.

85 FPT_TSA.2.4 The TSF shall be capable of distinguishing the set of users authorized for administrative functions from the set of all users of the TOE.

86 FPT_TSA.2.5 The TSF shall allow only specifically authorized users to assume the security administrative role.

87 FPT_TSA.2.6 The TSF shall require an explicit request to be made in order for an authorized user to assume the security administrative role.

FPT_TSM.1 Management Functions

88 FPT_TSM.1.1 The TSF shall provide the authorized administrator with the ability to set and update [security relevant databases], **and to require that users on the external network, internal network, or both, be authenticated prior to receiving services.**

89 FPT_TSM.1.2 The TSF shall provide the authorized administrator with the ability to perform [installation and initial configuration of the firewall; functions that allow system start-up and shutdown; backup and recovery]. **The backup capability shall be supported by automated tools.**

90 **If the TSF supports remote administration from either the internal or external interface, the TSF shall:**

a) Have the option of disabling remote administration on either or both interfaces.

b) Be capable of restricting the address from which remote administrator actions can be performed.

Requirements Overview:The remaining functional security requirements (Class FAU) deal with the need for producing, managing, protecting, and processing security audit information.

FAU_GEN.1 Audit Data Generation

91 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions.

b) All auditable events relevant for the *basic* level of audit defined in all functional components included in the PP/ST. **Included in Table 5.2**

c) Based on all functional components included in the PP/ST, *the events indicated as “extended” in Table 5.2*.

d) **Start of a session, connection attempts rejected by the firewall's access rules, authentication failures**.

92 FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, **object identity**, and *success or failure* of the event.

b) **Information specified in Table 5.2** for each audit event type, based on the auditable event definitions of the other functional components included in the Protection Profile and/or Security Target.:

Parent Family	**Level**	**Auditable event**
FAU_GEN	extended	Shutdown of the audit functions.
FAU_MGT	basic	Any attempt to perform an operation on the audit trail
FAU_POP	basic	Any specific operation performed to process audit data stored in the audit trail
FDP_ACC	extended	Decisions to permit a requested operation.
	extended	Decisions to deny a requested operation.
FDP_ACF	basic	Unsuccessful attempts to specify the granting or denying of access to an object
FDP_SAM	basic	All attempts to modify security attributes, including the identity of the target of the modification attempt and the new values of the modified security attributes.
	extended	The identity of a user and/or subject attempting to modify security attributes, and the target of the modification.
FDP_SAQ	basic	All attempts to query security attributes, including the identity of the target of the query.
FIA_ADA	basic	All requests to use TSF authentication data management mechanisms.
FIA_ADP	basic	All requests to access user authentication data.
FIA_AFL	extended	The termination of a session caused by a number of unsuccessful authentication attempts that exceed the threshold setting.
FIA_SOS.2	basic	Rejection or acceptance by the TSF of any tested secret.
FIA_UAU	basic	Any use of the authentication mechanism.
FIA_UID	basic	All attempts to use the user identification mechanism, including user identify provided.
FPT_TSA	basic	The allocation of a function to a security administrative role.
	extended	Use of a security-relevant administrative function.

Table 5.2 - Auditable Events

FAU_MGT.1 Audit Trail Management

93 FAU_MGT.1.1 The TSF shall provide the authorized administrator with the ability to *create, archive, delete, and empty* the audit trail.

FAU_POP.1 Human Understandable Format

94 FAU_POP.1.1The TSF shall provide the capability to generate human understandable presentation of any audit data stored in the permanent audit trail.

FAU_PRO.1 Restricted Audit Trail Access

95 FAU_POR.1.1 The TSF shall restrict access to the audit trail to the authorized administrator.

FAU_SAR.1 Restricted Audit Review

96 FAU_SAR.1.1 The TSF shall provide audit review tools, with the ability to view the audit data.

97 FAU_SAR.1.2 The firewall shall restrict the use of the audit review tools to the authorized administrator.

FAU_SAR.3 Selectable Audit Review

98 The TSF shall provide audit review tools with the ability to perform searches and sorting of audit data based on:

- [Subject ID;
- Object ID;
- Specific security conditions (e.g., rejected access requests);
- Accesses by specific subjects to specific objects;
- Access to specific objects by specific objects].

Application Note: The author of the ST is expected to describe the detailed capabilities of the audit review tools. In particular, the ability to search and sort based on security-relevant attributes must be described.

FAU_STG.3 Prevention of Audit Data Loss

99 FAU_STG.3.1 The TSF shall store generated records of audit in a permanent audit trail.

100 FAU_STG.3.2 The TSF shall limit the number of audit events lost due to *failure and attack*.

101 FAU_STG.3.3 In the event of audit storage exhaustion, the TSF shall be capable of *preventing* the occurrence of auditable actions, except those taken by the authorized administrator.

Application Note: It is expected that the firewall developer will provide an analysis of the maximum amount of audit data that can be expected to be lost resulting from failure or audit storage exhaustion.

5.1.2 ASSURANCE REQUIREMENTS

102 The assurance requirements levied on the developer consist of EAL2 and are summarized in the following table.

Assurance Class	Assurance Components
Configuration Management	ACM_CAP.1 Minimal Support
Delivery and Operation	ADO_IGS.1 Installation, Generation, and Start-up Procedures
Development	ADV_FSP.1 TOE and Security Policy
	ADV_HLD.1 Descriptive High-Level Design
	ADV_RCR.1 Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1 Administrator Guidance
	AGD_USR.1 User Guidance
Tests	ATE_IND.1 Independent Testing - Conformance
	ATE_COV.1 Complete Coverage - Informal
	ATE_DPT.1 Complete Coverage- Informal
	ATE_FUN.1 Functional Testing
Vulnerability Analysis	AVA_SOF.1 Strength of TOE Security Function Evaluation
	AVA_VLA.1 Developer Vulnerability Analysis

Table 5.3 - Assurance Requirements; EAL2

ACM_CAP.1 Minimal Support

103 ACM_CAP.1.1D The developer shall use a configuration management (CM) system.

104 ACM_CAP.2D The developer shall provide CM documentation.

105 ACM_CAP.1C The CM documentation shall include a configuration list.

106 ACM_CAP.2C The configuration list shall describe the configuration items that comprise the TOE, **and shall include the external network services that are used by the TOE**.

107 ACM_CAP.3C The CM documentation shall describe the method used to uniquely identify the TOE configuration items.

108 ACM_CAP.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, Generation, and Start-up Procedures

109 ADO_IGS.1.1.D The developer shall document procedures to be used for the secure installation, generation, and start-up of the TOE.

110 ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

111 ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1 TOE and Security Policy

112 ADV_FSP.1.1D The developer shall provide a functional specification.

113 ADV_FSP.1.2D The developer shall provide a TSP.

114 ADV_FSP.1.1C The functional specification shall describe the TSP using an informal style.

115 ADV_FSP.1.2C The functional specification shall include an informal presentation of syntax and semantics of all external TSF interfaces.

116 ADV_FSP.1.3C The functional specification shall include evidence that demonstrates that the TSF is completely represented.

Application Note: This requirement potentially can be met by a combination of documents, including the security target and external interface specification.

117 ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

118 ADV_FSP.1.2E The evaluator shall determine that the functional specification is consistent with the TSP.

119 ADV_FSP.1.3E The evaluator shall determine if the functional requirements in the Security Target are addressed by the representation of the TSFs.

ADV_HLD.1 Descriptive High-Level Design

120 ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

121 ADV_HLD.1.1C The presentation of the high-level design shall be informal.

122 ADV_HLD.1.2C The high-level design shall describe the structure of the TSF in terms of subsystems.

123 ADV_HLD.1.3C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

124 ADV_HLD.1.4C The high-level design shall identify the interfaces of the subsystems of the TSF.

125 ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

126 ADV_HLD.1.1E The evaluator shall conform that the information provided meets all requirements for content and presentation.

127 ADV_HLD.1.2E The evaluator shall determine if the functional requirements in the ST are addressed by the representation of the TSF.

ADV_RCR.1 Informal Correspondence Demonstration

128 ADV_RCR.1.1D The developer shall provide evidence that the least abstract TSF representation provided is an accurate, consistent, and complete instantiation of the functional requirements expressed in the ST.

129 ADV_RCR.1.1C For each adjacent pair of TSF representations, the evidence shall demonstrate that all parts of the more abstract representation are refined in the less abstract representation.

130 ADV_RCR.1.2C For each adjacent pair of TSF representations, the demonstration of correspondence between the representations may be informal.

131 ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

132 ADV_RCR.1.2E The evaluator shall analyze the correspondence between the functional requirements expressed in the ST and the least abstract representation provided to ensure accuracy, consistency, and completeness.

AGD_ADM.1 Administrator Guidance

133 AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

134 AGD_ADM.1.1C The administrator guidance shall describe how to administer the TOE in a secure manner.

135 AGD_ADM.1.2C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

136 AGD_ADM.1.3C The administrator guidance shall contain guidelines on the consistent and effective use of the security functions within the TSF.

137 AGD_ADM.1.4C The administrator guidance shall describe the difference between two types of functions: those which allow an administrator to control security parameters, and those which allow the administrator to obtain information only.

138 AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the administrator’s control.

139 AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

140 AGD_ADM.1.7C The administrator guidance shall contain guidelines on how the security functions interact.

141 AGD_ADM.1.8C The administrator guidance shall contain instructions regarding how to configure the TOE.

142 AGD_ADM.1.9C The administrator guidance shall describe all configuration options that may be used during secure installation of the TOE.

143 AGD_ADM.1.10C The administrator guidance shall describe details, sufficient for use, of procedures relevant to the administration of security.

144 AGD_ADM.1.11C The administrator guidance shall be consistent with all other documents supplied for evaluation.

145 AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

146 AGD_ADM.1.2E The evaluator shall confirm that the installation procedures result in a secure configuration

AGD_USR.1 User Guidance

147 AGD_USR.1.1D The developer shall provide user guidance.

148 AGD_USR.1.1C The user guidance shall describe the TSF and interfaces available to the user.

149 AGD_USR.1.2C The user guidance shall contain guidelines on the use of security functions provided by the TOE.

150 AGD_USR.1.3C The user guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

151 AGD_USR.1.4C The user guidance shall describe the interaction between user-visible security functions.

152 AGD_USR.1.5C The user guidance shall be consistent with all other documentation delivered for evaluation.

153 AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1 Independent Testing - Conformance

154 ATE_IND.1.1D The developer shall provide the firewall for testing.

155 ATE_IND.1.1C The firewall shall be suitable for testing.

156 ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_COV.1 Complete Coverage - Informal

157 ATE_COV.1.1D The developer shall provide an analysis of the test coverage.

158 ATE_COV.1.1C The analysis of the test coverage shall demonstrate that the tests identified in the test documentation cover the TSF.

159 ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional Testing

160 ATE_FUN.1.1D The developer shall test the TSF and document the results.

161 ATE_FUN.1.2D The developer shall provide test documentation.

162 ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, and test results.

163 ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

164 ATE_FUN1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function.

165 ATE_FUN.1.4C The test results in the test documentation shall show the expected results of each test

166 ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each security function operates as specified.

167 ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing - Functional Specification

168 ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

169 ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TOE operates in accordance with the functional specification of the TSF.

170 ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1 Strength of the TOE Security Function Evaluation[3]

171 AVA_SOF.1.1D The developer shall identify all TOE security mechanisms for which a strength of TOE security function analysis is appropriate.

172 AVA_SOF.1.2D The developer shall perform a strength of TOE security function analysis for each identified mechanism.

173 AVA_SOF.1.1C The strength of TOE security function analysis shall determine the impact of the identified TOE security mechanisms on the ability of the TOE security functions to counter the threats.

174 AVA_SOF.1.2C The strength of TOE security function analysis shall demonstrate that the identified strength of the security functions is consistent with the security objectives of the TOE.

175 AVA_SOF.1.3C Each strength claim shall be either basic, medium, or high.[4]

176 AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

177 AVA_SOF.1.2E The evaluator shall confirm that all TOE security mechanisms requiring a strength analysis have been identified.

178 AVA_SOF.1.3E The evaluator shall confirm that the strength claims are confirmed.

AVA_VLA.1 Developer Vulnerability Analysis

179 AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP. **This shall include a search for vulnerabilities identified in Appendix B.**

180 AVA_VLA1.2D The developer shall document the disposition of identified vulnerabilities.

181 AVA_VLA.1.1C The evidence shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.

3. AVA_SOF is intended to apply strictly to those security mechanisms that are amenable to attack as a result of quantitative or statistical analysis (e.g., passwords). A fuller discussion is provided in the Part 3 of the CC, in AVA_SOF, "Objectives."

182 AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

183 AVA_VLA.1.2E The evaluator shall conduct penetration testing, based on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 RATIONALE

6.1 RATIONALE FOR SECURITY OBJECTIVES

O.ACCESS

184 This security objective is necessary to counter threats T.SPOOF, T.SACCESS, and T.SOURCE.

O.ADMIN

185 This security objective is necessary to counter threats T.LACCESS and T.DCORRUPT.

O.IDENT

186 This security objective is necessary to counter threat T.LACCESS.

O.MINRES

187 This security objective is necessary to counter threat T.LACCESS.

O.PROTECT

188 This security objective is necessary to counter threats T.LACCESS and T.DCORRUPT.

O.AUDIT

189 This security objective is necessary to counter threats T.PENET, T.AUDITREV, and T.ACORRUPT.

[4] The definitions of “basic,” “medium,” and “high” are given in Part 3 of the CC under AVA_SOF, “Application Notes.”

6.2 RATIONALE FOR IT SECURITY REQUIREMENTS

FDP_ACC.2 Complete Object Access Control

190 This component was chosen to provide the basic definitions for the access control functionality of the firewall. This component directly supports the Access Control security objective, O.ACCESS, and supports O.MINRES.

FDP_ACF.2 Multiple Security Attribute Access Control

191 This component was chosen to provide the access control functionality of the firewall. This component directly supports the Access Control security objective, O.ACCESS, and supports O.MINRES.

FDP_ACF.4 Access Authorization and Denial

192 This component was chosen to require the ability to configure the access control functionality of the firewall; this actually allows the administrator to implement the policy. This component directly supports the Access Control security objective, O.ACCESS, and supports O.MINRES.

FDP_RIP.3 Full Residual Information Protection on Allocation

193 This component was chosen to avoid exposure of residual data in storage objects. This component supports the access control policy by guaranteeing that users do not accidentally acquire data not explicitly granted to them. This component supports O.ACCESS

FDP_SAM.1 Minimal Attribute Modification

194 This component was chosen to require that administrators be the only ones to have the ability to configure the access control functionality of the firewall. These are the only “attributes” that can be modified by administrators of the firewall (see application notes for more information on this model). This component directly supports the Access Control security objective, O.ACCESS. This component also supports Administrative Control security objective, O.ADMIN.

FDP_SAQ.1 Minimal Attribute Query

195 This component was chosen to allow the administrators the ability to view the access control rules they set up. This component directly supports the Administrative Control security objective, O.ACCESS.

FIA_ATA.1 User Attribute Initialization

196 This component is included to support the user identification and authentication objective, O.IDENT, by supporting the need for user attributes to be defined and initialized.

FIA_ADA.1 User Authentication Initialization

197 This component is included to support the need to initialize authentication data and to manage it over time in support of O.IDENT.

FIA_ATD.2 Unique User Attribute Definition

198 This component is included to support the dependency identified in FPT_TSA.1. It supports the need to define the shared attributes and directly supports the identification and authentication objective, O.IDENT.

FIA_ADP.1 Basic User Authentication Data Protection

199 This component is included to provide protection for user authentication data. Doing so is considered critical for satisfying security objectives, including O.IDENT.

FIA_AFL.1 Basic Authentication Failure Handling

200 This component is included to prevent repeated, undetected attempts to attack the firewall, especially attempts at guessing user IDs and passwords. It is a countermeasure for the threat T.LACCESS.

FIA_SOS.2 TSF Generation of Secrets

201 This component is included to provide support for strong authentication. Although strong authentication mechanisms offer considerable benefit in general, when compared to conventional authentication mechanisms (e.g., passwords), it is particularly important when the capability for remote administrator access is provided. This component directly supports the capabilities required under FPT_TSM.1

FIA_UAU.2 Single-use Authentication Mechanism

This component is intended to require the firewall to support one-time passwords. This component is included to provide direct support for user authentication.

FIA_UID.2 Unique User Identification

202 This component is included to support the dependencies identified in FPT_TSA.1 and FAU_GEN.1 and to support the identification objective, O.IDENT.

FPT_RVM.1 Non-Bypassability of the TSP

203 This component is fundamental to the implementation of security products, and is included to require the firewall to mediate each and every request for services and resources from network users. This is directly in support of the Access Control security objective, O.ACCESS.

FPT_SEP.1 TSF Domain Separation

204 This component is included to ensure that the firewall itself is protected from attack by untrusted subjects. Because of this, this component has to be included to ensure the firewall can protect itself should it offer this additional functionality. Although this means that FPT_SEP.1.2 is essentially meaningless (or trivially satisfied) for pp-compliant firewalls, the same cannot be said for FPT_SEP.1.1. This component supports the Firewall Self-Protection security objective, O.PROTECT.

FPT_TSA.2 Separate Security Administrative Role

205 This component is included to provide a means to administer the security functions of the firewall, and to control the exercise of administrative functions by supporting a distinct administrator role. This component is directly in support of the Administrative Control security objective, O.ADMIN.

FPT_TSM.1 Management Functions

206 This component further specifies the abilities necessary to successfully and securely administer the firewall. This component is directly in support of the Administrative Control security objective, O.ADMIN.

FAU_GEN.1 Audit Data Generation

207 This component is included to specify the particular types of audit events, as well as minimal content for the audit records, for pp-compliant firewalls. Note that only “failure” events need to be auditable in FAU_GEN.1.2.a, so the amount of

information that is required should be manageable. This component directly supports the Audit security objective, O.AUDIT.

FAU_POP.1 Human Understandable Format

208 Audit data are useless unless there is some means to view them; this component requires that they be viewable. This component directly supports the Audit security objective, O.AUDIT.

FAU_PRO.1 Restricted Audit Review

209 This component is included to restrict access to the review tools. This component directly supports the Audit security objective, O.AUDIT.

FAU_MGT.1 Security Audit Management

210 This component is included to further define the requisite audit trail management capabilities. This component directly supports the Audit security objective, O.AUDIT.

FAU_SAR.1 Selectable Audit Review

211 This component requires that tools be available for viewing audit data, and that the use of these tools be restricted to the authorized administrator. This component directly supports the Audit security objective, O.AUDIT.

FAU_SAR.3 Security Audit Event Selection

212 This component specifies that a limited search and sort capability must be present; because of the volume of audit data, this requirement makes perfect sense. This component directly supports the Audit security objective, O.AUDIT.

FAU_STG.2 Enumeration of Audit Data Loss

213 This component not only satisfies dependencies generated by the audit reporting requirements, but also includes a limit as to the number of audit records lost due to both failure and attack; important to support the Audit security objective with respect to maintaining a relatively complete audit record, O.AUDIT.

6.3 RATIONALE FOR ASSURANCE REQUIREMENTS

214 EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor. As such, minimal additional tasks are imposed upon the vendor to the extent that if the vendor applies reasonable standards of care to the

development, evaluation may be feasible without vendor involvement other than support for functional testing. The chosen assurance level should satisfy all functional dependencies, and is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

Appendix A

TSF Generation of Secrets

Implementations of any of the following standards satisfy the requirements of FIA_SOS.2:

- Digital Signature Standard [FIPS PUB 196]

Note: ***The authors request that readers submit other standards or generic descriptions of other acceptable products (i.e., not implementation-specific) to be considered for inclusion in this list.***

Appendix B

Vulnerability List for AVA_VLA.

The search for obvious vulnerabilities required by AVA_VLA.1.D shall include, but is not limited to, a search for the following vulnerabilities:

ftp daemon vulnerabilities

Description:

In certain versions of the ftp daemon, a vulnerability exists allowing local and remote users to gain root privileges. This is accomplished through different means for distinct version such as through the signal handling routine increasing process privileges or through exploiting the SITE EXEC command.

See the Addendum for the relevant CERT advisory summaries (CA-97:16, CA-95:16, CA-94:08).

IMAP and POP server vulnerability

Description:

In certain versions, both IMAP and POP servers are vulnerable when remote users attempt to perform off-line mail processing. Remote clients connecting to these servers must login. A vulnerability exists in the handling of these logins resulting in privileged access to the server.

See the Addendum for the relevant CERT advisory summary (CA-97:09).

InterNet News daemon attacks

Description:

The inn daemon passes some control information to the mailer on the system without checking the contents. The mailer then passes the contents to the shell to be executed using the shell’s “eval” command. The shell script executes with the authority of the inn daemon and thus permits anyone who can send messages to this inn server to execute arbitrary commands.

See the Addendum for the relevant CERT advisory summary (CA-97:08).

http daemon vulnerabilities

Description:

Any http server which has installed CGI programs that rely on the escape_shell_cmd() library function to prevent exploitation may be vulnerable. Remote users can execute arbitrary commands and create files with the privileges of the http daemon.

A second http-related vulnerability exists in some nph-test-cgi scripts with some http daemons. Remote users without an account on the system can gain read access to files they should not be capable of reading because the cgi script parses data requests too liberally.

A third http-related vulnerability allows certain http daemons to execute arbitrary shell commands on behalf of unauthorized remote users with the privileges of the http daemon.

See the Addendum for the relevant CERT advisory summaries (CA-97:07, CA-96:06, CA-95:04).

rlogin with TERM environment variable vulnerability

Description:

If, during an rlogin attempt on certain vulnerable systems, the buffer containing the value of the TERM environment variable is overflowed, arbitrary code can be executed as root.

See the Addendum for the relevant CERT advisory summary (CA-97:06).

Sendmail vulnerabilities

Description:

Remote users may be able to execute arbitrary commands with root privileges on systems receiving mail that are running a vulnerable version of sendmail that support MIME.

A second vulnerability to certain versions of sendmail occurs when an attacker gains group permissions of another user. This is possible when mail is sent to a users .forward or :include: file which is located in a directory that is writable by the attacker.

A third vulnerability to certain versions of sendmail occurs when users other than root invoke sendmail in daemon mode, bypassing code intended to prevent this.

A fourth vulnerability to certain versions of sendmail occurs when buffer overflows lead to unauthorized users gaining root access.

A fifth vulnerability to certain versions of sendmail occurs in the case of resource starvation. A user with an account can exploit sendmail when sendmail cannot distinguish between a “resource failure” and “user id not found” error. Starving sendmail will create files owned by the “default user” which can then be used to gain access to other files owned by that user.

See the Addendum for the relevant CERT advisory summaries (CA-97:05, CA-96:25, CA-

96:24, CA-96:20).

IP Spoofing attacks

Description:

Firewalls are vulnerable to IP spoofing attacks, including TCP SYN Flooding attacks. Firewalls should have a mechanism to handle SYN Flooding attacks. Firewalls should be capable of preventing traffic from entering the protected local network when packets claim to originate from local network, broadcast network, reserved network, or loopback network addresses.

See the Addendum for the relevant CERT advisory summary (CA-96:21).

rpc vulnerabilities

Description:

A vulnerable version of rpc.pcnfsd allows remote users to execute arbitrary commands with root privileges.

A vulnerability exists in versions of rpc.statd where it does not validate the information received from rpc.lockd. Thus, rpc.statd can then be made to remove or create files on the NFS server with root privileges.

A vulnerability in certain versions of rpc.ypupdated, resulting from a failure to check whether a client has update access to NIS data, can allow arbitrary commands to be executed on NIS servers.

See the Addendum for the relevant CERT advisory summaries (CA-96.09, CA-96:08, CA-95:17).

UDP attacks

Description:

Tools exist to flood UDP ports with packets causing degradation in system performance and increased network congestion. Firewalls must be capable of being configured to filter all UDP services.

See the Addendum for the relevant CERT advisory summary (CA-96:01).

Telnet Environment Option vulnerability

Description:

If the system to which the telnet connection attempt is directed is running telnet daemons that are RFC 1408 or RFC 1572 compliant and the system supports shared object libraries then the system may be vulnerable. Both users with and without accounts on the system could become root by transferring environment variables that influence the login program called by the telnet daemon.

See the Addendum for the relevant CERT advisory summary (CA-95:14).

NFS vulnerabilities

Description:

NFS is vulnerable when the portmapper port and the nfsd port are accessible. The Firewall should filter these ports and also prevent the portmapper from having proxy access, otherwise RPC services will be vulnerable in addition to NFS.

See the Addendum for the relevant CERT advisory summary (CA-94:15).

tftp daemon attacks

Description:

Remote users on the Internet may access world-readable files on an internal network using an unrestricted tftp service. Thus sensitive files could be retrieved by an adversary on the external side of the corporate firewall.

See the Addendum for the relevant CERT advisory summaries (CA-91:19, CA-91:18).

IP loose source route option vulnerability

Description:

Firewalls should be capable of rejecting packets that use the IP loose source route option. A malicious attacker can impersonate a host that is on the return path for this type of TCP traffic since the traffic must follow the reverse order of the route which it followed from source to destination.

See the Addendum following the CERT advisory summaries for more information.

RIP vulnerability

Description:

Injecting bogus RIP packets into a network will often be believed by routers even though there is no authentication field. This could cause traffic to be lead away from the intended destination by an attacker between the source and destination hosts.

See the Addendum following the CERT advisory summaries for more information.

ARP vulnerability

Description:

A vulnerability occurs as a result of the way the ARP protocol works. Because any host can respond to an ARP request, a malicious user could respond to the sender faster than the intended recipient of the ARP request. Thus, the malicious user will receive traffic that should have a different destination.

See the Addendum following the CERT advisory summaries for more information.

DNS vulnerabilities

Description:

Vulnerabilities exist in certain DNS implementations such that malicious users can gain access. Problems with DNS include the servers inability to handle a flood of DNS responses, the way in which the DNS resolver resolves different levels, and a target host performing a DNS cross-check after its DNS responses cache was previously maliciously altered.

References

[1] *Common Criteria for Information Technology Security Evaluation*, CCEB-96/011, Version 1, dated 96/01/31.

[2] *Network/Transport Packet Filter Firewall (PFFW) PP*; Common Criteria, Version 1.0, Part 4: Predefined Protection Profiles.

[3] Cheswick, William. R. and Bellovin, Steven M.; *Firewalls and Internet Security: Repelling the Wily Hacker,* Addison-Wesley Publishing Company, 1994

Acronyms

The following abbreviations from the Common Criteria are used in this Protection Profile:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Addendum

Vulnerability Summaries

The following consists of vulnerabilities derived from CERT advisories and summaries of other known vulnerabilities.

I. CERT ADVISORIES

CA-97:16 - ftpd Signal Handling Vulnerability

The signal handling routine causes this vulnerability by increasing a remote users’ process privileges to root, while continuing to catch other signals. This creates a race condition allowing anonymous as well as regular ftp users to gain root access. This allows users to read or write arbitrary files to the server.

CA-97:09 - Vulnerability in IMAP and POP

IMAP and POP support off-line mail processing. A client uses off-line mail processing when the client wishes to download mail that the server is holding for that client to the client’s local machine. In both protocols, IMAP and POP, the server runs with root privileges so it can access mail folders and perform necessary file manipulation on behalf of the remote user logging in. After logging in the root privileges are dropped. The vulnerability exists in the manner in which logins are handled. This can be exploited, giving the user logging in to the server root access on it. Carefully prepared text submitted during the login to the system running the vulnerable version of IMAP or POP can cause system buffers to overflow and execute arbitrary commands with root privileges.

CA—97:08 - innd Vulnerability

All versions of INN (InterNetNews) through 1.5 are vulnerable. The vulnerability which allows unauthorized users to execute arbitrary commands on machines running INN by sending maliciously formed news control messages should be prevented. These attacks can be launched remotely and may reach news servers behind the firewall.

The INN daemon (innd) processes "newgroup" and "rmgroup" control messages in a shell script (parsecontrol) that uses the shell's "eval" command. Some of the information passed to eval comes without adequate checks for characters that are special to the shell. This permits anyone who can send messages to an INN server - almost anyone with Usenet access - to execute arbitrary commands on that server. These commands run with the uid and privileges of the innd process on that server. Because such messages are usually passed through Internet firewalls to a site's news server, servers behind such firewalls are vulnerable to attack. Also the program executes these commands before checking whether the sender is authorized to create or remove newsgroups so checks at that level (such as running pgpverify) do not prevent this problem.

CA-97:07—httpd nph-test-cgi script Vulnerability

A vulnerability in the nph-test-cgi script included with some http daemons makes it possible for users of Web clients to read a listing of files they are not authorized to read without having an account on the system. This script is designed to display information about the web server environment. But it parses data requests too liberally and thus allows a person to view a listing of arbitrary files on the web server host.

Since this script is not required to run httpd successfully, this script should either be removed or the execute permissions should be removed. Note that web servers may have multiple cgi-bin directories, so it is not sufficient to look in the normal location only. Note that there may be other test cgi scripts that are also not required to run httpd successfully and are not intended to be left on an operational server.

CA-97:06— rlogin with TERM environment variable Vulnerability

Many implementations of the rlogin program contain a defect whereby the value of the TERM environment variable is copied to an internal buffer inappropriately. The buffer holding the copied value of TERM can be overflowed. In some implementations, the buffer is a local variable, meaning that the subroutine call stack can be overwritten and arbitrary code executed. The arbitrary code executed is under the control of the user running the rlogin program.

Since the rlogin program is set-user-id to root in order for it to have the server allocate a port in the range of 0-1023, this programming defect can be exploited to execute arbitrary code as root.

CA-97:05— MIME Conversion Buffer Overflow in Sendmail vers 8.8.3 and 8.8.4 Vulnerability

Sendmail can be configured on a mailer-by-mailer basis for either 7-bit ASCII or 8-bit MIME according to flags set defined by the mailer. MIME conversion of email is usually done on final delivery.

Sending carefully crafted email messages to a system running either version 8.8.3 or 8.8.4 of sendmail, intruders may be able to force sendmail to execute arbitrary commands as root. Intruders can do this without having an account.

The restricted shell program of sendmail should be used with all versions of sendmail. Using this gives you improved administrative control over the programs that sendmail executes on behalf of users.

If you run /bin/mail based on BSD 4.3 UNIX, replace /bin/mail with mail.local, which is included in the sendmail distribution. As of Solaris 2.5 and beyond, mail.local is included in the standard distribution.

Although the current version of mail.local is not the perfect solution to sendmail problems, it does counter known vulnerabilities that are being exploited. For more details, see CA-95:02.

Leaving executable copies of older versions of sendmail installed elsewhere (such as in /usr/lib), allows vulnerabilities in those versions to be exploited if an intruder gains access to your system. Either delete these versions or change the protections on them to be non-executable.

Similarly, if you replace /bin/mail with mail.local, remember to remove old copies of /bin/mail or make them non-executable.

CA-97:04—talkd, otalkd, ntalkd Vulnerability

As part of the talk connection, talkd does a DNS lookup for the name of the host that the connection is being initiated from. Because there is insufficient bounds checking on the buffer where the hostname is stored, it is possible to overwrite the internal stack space of talkd.

It is possible to force talkd to execute arbitrary commands by carefully manipulating the DNS hostname information. As talkd runs with root privileges, this may allow intruders to remotely execute arbitrary commands with these privileges.

CA-96:26—Denial of Service attack via ping

The TCP/IP specification allows for a maximum packet size of up to 65536 octets. It is known that some systems will react in an unpredictable fashion, including crashing, freezing, and rebooting, when receiving oversized IP packets.

In particular, Internet Control Message Protocol (ICMP) ECHO_REQUEST and ECHO_RESPONSE messages, used by a local host to determine whether a system is reachable via the network, issued via the ping program have been used to trigger this behavior.

The firewall shall be able to handle oversized ICMP datagrams without resulting in a denial of service.

CA-96:25—Version 8 sendmail Group Permissions Vulnerability

When version 8 of sendmail causes mail to be delivered to a program listed in .forward or :include:, that program is run with the group permissions possessed by the user owning that .forward or :include: file.

It is possible for users to obtain group permissions they should not have by linking to a file that is owned by someone else, but on which they have group write permissions. By changing that file, users can acquire group permissions of the owner of that file.

Exploitation is possible if the attacked user has a file that is group writable by the attacker on the same file system as either the attacker's home directory, or an :include: file that is referenced directly from the aliases file and is in a directory writable by the attacker. The first .forward attack works only against root. This attack does not give users root "owner" permissions, but does give them access to the groups that list root in /etc/group.

CA-96:24—Sendmail daemon mode vulnerability

Sendmail is often run in daemon mode so that it can "listen" for incoming mail connections on the standard SMTP port. The root user is the only user allowed to start sendmail in this way, and sendmail contains code intended to enforce this restriction.

Sendmail can be invoked in daemon mode bypassing the built-in check. When the check is bypassed, any local user can start sendmail in daemon mode. And as of version 8.7, sendmail will restart itself after receiving a SIGHUP signal. It will re-execute itself as root, using the exec system call. Thus, by manipulating the sendmail environment, the intruder can then have sendmail execute an arbitrary program as root.

CA-96:21—TCP SYN Flooding and IP Spoofing Denial of Service Attacks

The firewall shall be thoroughly examined to see how it handles TCP SYN Flooding attacks. This occurs when there are too many half-open connections (the server has sent a SYN-ACK and is waiting for the client to send an ACK back to the server). When the data structure available for handling pending connections fills up with too many pending connections, all new connection attempts will be refused. Normally, there is a timeout associated with a pending connection, however the attacker can just send connection requests faster than the server can clear the expired half-open connections in the structure.

IP Spoofing Attacks

Though these cannot be stopped entirely, the firewall must be capable of being set up to restrict packets to the external interface by not allowing a packet through if it has a source address from the internal network(s). In addition, the firewall shall be capable of recognizing and filtering outgoing packets that have a source address different from the internal network(s) to prevent source IP address spoofing from originating on the internal network.

The firewall's input filter should also be capable of filtering packets that come from Broadcast Networks (both the all 0's and all 1's broadcast networks), and these private reserved networks: 127.0.0.0 - 127.255.255.255 (loopback) 10.0.0.0 - 10.255.255.255 (reserved) 172.16.0.0 - 172.31.255.255 (reserved) 192.168.0.0 - 192.168.255.255 (reserved)

Turning off IP source routing, though recommended, will not stop IP spoofing attacks.

CA-96:20—2 sendmail Vulnerabilities up to and including version 8.7.5

Buffer Overflows

There are several buffer overflows present in sendmail version 8.7.5 and earlier. Some of the buffer overflows could result in local users gaining unauthorized root access. This must be prevented.

Resource Starvation

Anyone with access to an account on the system can run programs or write files as the default user. The danger of compromising the default user depends primarily on the other files in your system owned by that user.

CA-96:13—dip Program Vulnerability-

The dip program manages connections needed for dial up links such as SLIP and PPP. It can handle both incoming and outgoing connections. To gain access to these connections, it must be installed with setuid root.

A vulnerability in dip makes it possible to overflow an internal buffer whose value is under the control of the user of the dip program. If this buffer is overflowed with the appropriate data, a program such as shell can be started and will run with root permissions.

Thus on a system that has dip installed as setuid root, anyone with access to an account on that system can gain root access.

CA-96:11—Interpreters in cgi-bin directories

CGI programs are often scripts that are run by general purpose interpreters, such as /bin/sh or PERL. If these interpreters are in the cgi-bin directory along with the associated scripts, intruders can access the scripts directly and execute arbitrary commands on the web server's system. Note that the directory for CGI programs is typically cgi-bin, but the server may be configured to use a different name.

The solution to this problem is to ensure that the CGI bin directory does not include any general-purpose interpreters such as PERL, Tcl, any UNIX shells (sh, ksh, csh, etc.). etc.

CA-96:10—NIS+ Configuration Vulnerability

In vulnerable installations of NIS+, the access rights on the NIS+ passwd table are left in an unsecure state. This vulnerability is known to exist on Solaris 2.5 servers and similar vulnerabilities may exist in previous versions of Solaris 2, but should be checked in all systems.

This vulnerability may allow any user with login access to a client or server that uses NIS+ for authentication to gain root access.

CA-96:09—rpc.statd Vulnerability

The vulnerability is that files removable by root can be removed by rpc.statd. Also files that root could create can be created by rpc.statd with mode 200.

CA-96:08—pcnfsd (or rpc.pcnfsd) Vulnerabilities

One vulnerability is that local users can change the permissions on any file accessible to the local system that the root user can change. The second vulnerability is that remote users can execute arbitrary commands as root on the machine running pcnfsd.

CA-96:07—Java Development Kit (JDK) versions 1.0 and 1.0.1 Bytecode

Verifier Vulnerability

When viewing applets written with malicious intent, those applets can perform any operation that the legitimate user can perform on the machine running the browser or appletviewer.

CA-96:06—NCSA httpd 1.5a-export and APACHE httpd 1.0.3 Server CGI example Vulnerability

Any program relying on escape_shell_cmd() (in cgi-src/util.c) to prevent exploitation of shell-based library calls may be vulnerable to attack. Thus any program using this function should be disabled by removing the program or revoking the execute permissions to it. In particular, since the "phf" program is not required to successfully run the httpd, it should also be disabled.

CA-96:05—Java Development Kit (JDK) 1.0 and Netscape Navigator 2.0 Allow Connections to Arbitrary Hosts

The restriction allowing an applet to connect only to the host from which it was loaded needs to be properly enforced. The Applet Security Manager allows an applet to connect to any of the IP addresses associated with the computer from which it came. Java applets can connect to arbitrary hosts on the Internet, including those presumed to be previously inaccessible, such as hosts behind a firewall. Bugs in any TCP/IP based network service can then be exploited as well as services behind the firewall which had been thought to be secure.

CA-96:04—Corruption of Data From Network Information Servers Such as the Domain Name Service (DNS), YP, NIS, NIS+, and netinfo

Programs must check data provided by information servers such that these programs do not operate in unpredictable ways, giving unpredictable results. In particular, exploitation of this vulnerability may allow remote access by unauthorized users. It may also lead to root access by both local and remote users.

For example, programs that use the host name returned by gethostbyname() may use an information server that is beyond your control, and the data returned could be of the form that would cause a system() or popen() system calls to execute commands other than the one specified in the program.

CA-96:02—BIND Version 4.9.3 Vulnerability

Though the Berkeley Internet Name Domain (BIND) is an implementation of DNS that fixes several security flaws known to be exploited to render DNS information unreliable, it still can be spoofed into providing incorrect name data.

CA-96:01 - UDP port Denial of Service Attack

Hacker programs exist to cause "UDP Packet Storms." When the packet storm is directed at a single host this causes the host's performance to degrade. When the packet storm is between two hosts this causes not only each host's performance to degrade, but also causes extreme network congestion. For example, by connecting a host's chargen service to the echo service on the same or different machine, the effected machine(s) perform(s) poorly.

The firewall shall be capable of filtering UDP services, especially chargen and echo. All UDP ports less than 900 shall be capable of being filtered. We recommend that the firewall filter all unused UDP services.

CA-95:17—rpc.ypupdated Vulnerability

Clients connect to the rpc.ypupdated server that updates the NIS information database with information to update. The protocol used when clients connect to the rpc.ypupdated server checks that the connection is authentic but does not check to see if the client is authorized to modify the NIS data or if the included NIS map exists. Even after an unsuccessful attempt to update the NIS information, the rpc.ypupdated server invokes the make(1) program to propagate possible changes. The implementation of make is not secure which may allow the requesting client to pass malicious arguments resulting in the execution of arbitrary commands on NIS master and slave servers.

CA-95:16 - Improper configuration of the SITE EXEC ftp daemon command

Certain configurations of the SITE EXEC command in the systems ftp server are vulnerable to attack. The problem is that the variable _PATH_EXECPATH was set to "/bin" in the configuration file, when it should be set to "/bin/ftp-exec" or some similar directory that does not contain a shell or command interpreter. Only a user with a local account on such an improperly configured system offering the ftp service may gain root access.

CA-95:14—Telnetd Environment Option Vulnerability

If the remote or targeted system where a telnet is connecting runs an RFC 1408 or RFC 1572 compliant telnet daemon and the targeted system also supports shared object libraries, then it may be vulnerable to attack. It may be possible to transfer environment variables that influence the login program called by the telnet daemon. A user may then bypass the normal login and authentication scheme and may become root on that system.

Thus if such a telnet daemon is vulnerable, it should be replaced with one that changes the environment given to the login program.

CA-95:13—Syslog Vulnerability

The syslog(3) subroutine uses an internal buffer for building messages that are sent to the syslogd(8) daemon. This subroutine does no range checking on data stored in this buffer. It is possible to overflow the internal buffer and rewrite the subroutine call stack. It is then possible for local and remote users to execute arbitrary programs. Several programs use the syslog subroutine including, sendmail, httpd, ftpd, and telnetd. All these and other programs that use syslog are vulnerable to this problem.

CA-95:08—Sendmail Version 5 Vulnerability

Users of Version 5 sendmail that have not upgraded are vulnerable. Local and remote users can create files, append to existing files or run programs on the system. Exploitation of this vulnerability can lead to root access.

CA-95:04— NCSA HTTP Daemon Version 1.3 for UNIX Vulnerability

Version 1.3 (and some earliers versions) of the NCSA HTTP Daemon can be tricked into executing shell commands. Thus users without a local account may gain unauthorized access to the account under which the httpd process is running.

CA-94:15—NFS Vulnerabilities

Intruders have widely available and widely distributed tools available to exploit NFS vulnerabilities. To prevent access to NFS at the internal network the firewall must filter TCP and UDP port 111 (the portmapper). Also to prevent access to NFS at the internal network, the firewall must filter the nfsd port (typically TCP and UDP port 2049).

Note that NFS will sometimes run on a different port. If NFS is running on a different port then that is the correct nfsd port to filter. Note also that this measure does not prevent attacks from inside the internal network on NFS.

The portmapper should disallow proxy access to protect all hosts from portmapper attacks that originate from both inside and outside the firewall. As a result, since systems on the internal network may be running vulnerable RPC services, blocking the portmapper port would prevent these RPC services from being found by intruders.

CA-94:08—ftpd SITE EXEC Vulnerability

Some implementations of ftpd that support the SITE EXEC command feature of the ftpd daemon are vulnerable in that a local or remote user can gain root access. The SITE EXEC feature must be explicitly activated in order to be exploited. There is also a race condition in certain implementations that also leads to root access.

CA-93:14 - Internet Security Scanner

Accounts on the Firewall:

All default accounts (e.g., guest, bbs, etc.) as well as the lp account, if they exist, must be disabled by replacing the encrypted password with a "*" in the password file. Additionally, the string "/bin/false" should be added to the shell field in the password file.

Decode Alias:

Mail aliases for decode and uudecode must be disabled on UNIX systems

Sendmail Commands "wiz" and "debug":

The sendmail commands "wiz" and "debug" must be disabled. If the "wiz" command returns "Please pass, oh mighty wizard" the system is vulnerable to attack. Systems that return "200 Debug set" from the "debug" command are also vulnerable.

Mounting File Systems Under NFS:

File systems exported under NFS should be mountable only by a restricted set of users. If any file system is currently mountable by "everyone" then this must be change to restrict access to that partition.

Displaying User Account Information Using rusers Server:

The rusers server should be disabled because the information received from it could be used by an attacker to determine account names or other useful information to mount an attack.

Remote Execution Server rexd:

The UNIX remote execution (rexd) server provides only minimal authentication and is easily subverted. It should be disabled to prevent an attack through this server.

Source Port Set Up To Bypass Firewall:

A firewall must prevent unauthorized connection through ports that exist to allow certain applications to work. This provides intruders access to machines on the internal network and bypasses the firewall's security mechanisms. For example, when used as a source port for TCP connections, FTP-DATA port 20 on some improperly configured firewalls may allow the firewall to be bypassed.

CA-91:18—tftp Internet attacks Vulnerability

CA-91:19—IBM AIX TFTP Daemon Vulnerability

Unrestricted tftp access allows remote sites to retrieve copies of any world-readable files. Use of unrestricted tftp would allow anyone on the Internet to retrieve copies of a sites sensitive files such as /etc/passwd. The intruder could later crack the password file and use the information to login to accounts. This may provide root access.

The tftp protocol should be filterable by the firewall or a file writable only by root (such as /etc/tftpaccess.ctl) shall exist on systems on the inside network to restrict the files that should be accessible. Firewalls configured to allow tftp access shall make the possible dangers of its use clear in the documentation.

II. OTHER VULNERABILITIES

IP loose source route option vulnerability

A TCP connection where the loose source route option is enabled allows an attacker to explicitly route packets through the network to a destination without following the usual routing process. RFC 1122 specifies that packets must follow the same route on the return path. An malicious user could then pose as one of the hosts in the return path. Firewalls should be capable of rejecting loose source routed packets.

RIP vulnerability

As a result of the ease with which bogus RIP packets may be injected into a network, packets can be lead away from their intended destination if the attacking host is closer to the target than the valid sending host. This occurs when routers accept RIP packets and because RIP performs no type of authentication. Firewalls should be configured to disallow routing along certain links such as intermediate links on an external network while the source and destination hosts are both on the internal network.

ARP vulnerability

A malicious host can send false ARP responses back to the sender before the true recipient receives the ARP request and responds back. Thus the sender will now be fooled into sending traffic to the malicious host in the middle rather than the proper destination host. The malicious host can either impersonate the destination host, or intercept, modify, and resend the traffic to the sending host’s intended destination. Firewalls should not allow ARP requests to pass through them and should not perform proxy ARP for requests from an external network.

DNS vulnerabilities

A flood of DNS responses injected into the network could cause a denial of service since the DNS server may become confused.

A DNS resolver may check several different levels before checking the correct one. If a host, FOO.BAR.COM, attempts to connect to ONE.TWO, the check will be made first to ONE.TWO.BAR.COM and then to ONE.TWO.COM and finally to ONE.TWO. Thus a malicious host can impersonate a domain that the resolver would encounter before encountering the appropriate level.

If an attacker can contaminate a target’s DNS responses cache before the call is made, the target can be fooled into believing that the cross-check it performs is legitimate. As a result, the attacker gains access.

Comment Format

Firewall Comment Format

1: Originator Name

2: Originator organization

3: Return address

4: Date

5: Referenced Section/Paragraph

6: One line summary/title of observation

7: Comment/Observation

8: Suggested solution